Microsoft

Leveraging Security Features in Windows 2000 for Exchange

For IT administrator

Abstract

This white paper describes the features of Microsoft® Windows® 2000 and how Microsoft Exchange 2000 Server takes advantage of them. These features include Kerberos-based authentication, granular authorization system, auditing system, certificate services, and others. This document explains the interoperability of these systems with other platforms so that users can build a security-conscious architecture. It also discusses security for both internal LAN and external networks.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

CONTENTS

INTRODUCTION....4

ACTIVE DIRECTORY....5

Active Directory Connectors 6
Extension of the Active Directory Schema by Exchange 8

KERBEROS....11

Introduction 11
Kerberos and Exchange 11
Authentication Delegation in Exchange 13
Kerberos for Non-Windows 2000 clients 13
Best Practices 14

ACCESS CONTROL....15

Item Level and Property Level 17
Planning Considerations 17
Directory-Level Delegation 18
Exchange Roles 20

CERTIFICATE SERVICE....22

Certificate Service and Active Directory 22
Certificate Service and KMS 22

IP SECURITY (IPSEC)....26

IPSEC and SSL 26
Using IPSEC in LAN 26
IPSEC and Exchange 28

OTHER SECURITY ENHANCEMENTS....30

Encrypting File System (for the Client PC) 30
Auditing in Windows 2000 31

FINAL NOTES....33

Two Broad Areas of Security 34
Internal Security 34
External Security 34
PORTS and PROTOCOLS Used 34
Location Service 35
NetBIOS Name Service 35
Remote Access and VPN 36
Lowest Common Denominator 37

For More Information....38

INTRODUCTION

This paper explains the different features in Microsoft Windows® 2000 and how Microsoft Exchange 2000 Server takes advantage of them. These new features are not found in previous versions of Microsoft Windows NT® servers. They define a new environment in which the enterprise messaging and collaborative system operate. It is necessary to understand these features, because users need to know how the systems behave in other platform environments.

These features in Windows 2000 can be broadly divided into two areas: core operating system features and additional security features.

Windows 2000 integrates core operating system features that form the basis of a secured implementation. They are:

- Active Directory™ directory service – object unification of the Exchange directory and the Windows 2000 directory
- Kerberos – authentication
- Access Control Model – detailed control over of Active Directory entries and Exchange objects
- Microsoft Certificate Services – used by other applications to provide security across different layers

There are security applications that can further enhance the security of the enterprise. These applications make use of the core operating system features. They are:

- IP Security (IPSEC) – used in LAN, remote access, and Virtual Private Network (VPN)
- Encrypted File System – provides additional security for mobile users
- Security Configuration Analyzer –ensures adherence to security policies

This paper also explores two broad areas in which these features can be harnessed extensively: a LAN and an environment where one network connects to the other. It looks at the options available for a secured environment.

ACTIVE DIRECTORY

Active Directory in the domain controller replaces the Security Accounts Manager (SAM) in Windows NT 4.0 as the security database. Every object in Active Directory that takes part in any security process needs to have a Security Identifier (SID). A SID is a pseudorandom identifier that is a globally unique, 96-digit number to identify users and computers.

There are two different sets of objects on Windows NT 4.0 and Exchange 5.5. For instance, the directory for Exchange is separate from the directory structure of Windows NT 4.0. However, these are unified in Active Directory and hence reduce administrative tasks. Essentially, the objects in Exchange 2000 and Windows 2000 are linked to a SID. Custom recipients in Exchange 5.5 are mail-enabled contacts in Exchange 2000 and do not have a SID. Distribution lists are changed to groups. There are security groups with a SID and distribution groups without a SID. When an object does not have a SID, the object cannot be placed in the access control list.

Exchange 5.5 Recipient	**Windows 2000 Active Directory Object**
Mailbox	A mailbox is a mailbox-enabled user. An e-mail address shows the Exchange server where the e-mail is to be routed. Mailboxes from Exchange 5.5 are replicated into Active Directory as users or contacts.
Distribution Lists	A distribution list is a group. Windows 2000 groups appear as distribution lists in an Exchange directory. The administrator can specify the group to be a security group, which allows the group to be placed in an access control list. Figure 1 shows a Microsoft Outlook® discussion group that has the Distribution check box enabled and an e-mail address.
Custom Recipients	A mail-enabled contact is a custom recipient in an Exchange directory. It has an e-mail address associated with it but not an Exchange mailbox. It does not have a SID and cannot log on.

Table 1 shows how Exchange 2000 in Active Directory represents the objects in Exchange 5.5.

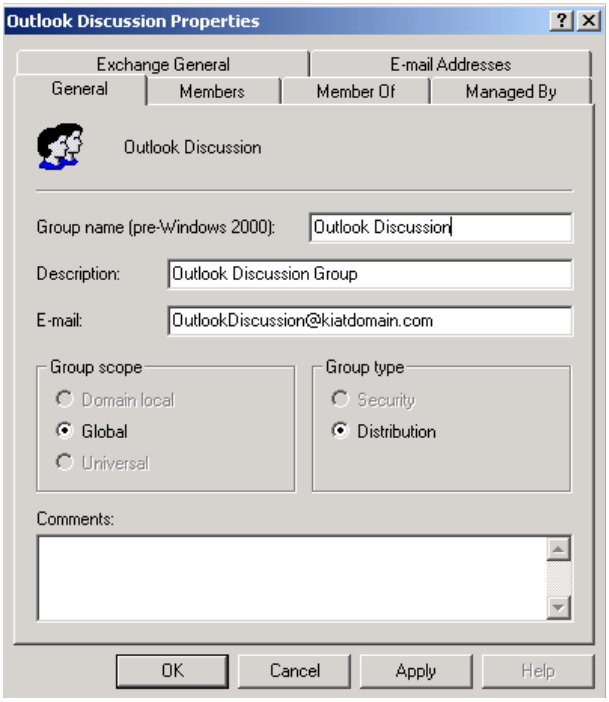


Figure 1 shows the user interface (UI) for configuring an outlook discussion property as a distribution group.

Windows 2000 defines various types of objects that can be hosted in Active Directory.

Mail-Disabled	Has no e-mail capabilities. A security group like Domain Admins is an example.
Mail-Enabled	Has an e-mail address but no mailbox. A distribution group is an example.
Mailbox-Enabled	Has an Exchange mailbox associated with it and only Windows user accounts can be mailbox-enabled.

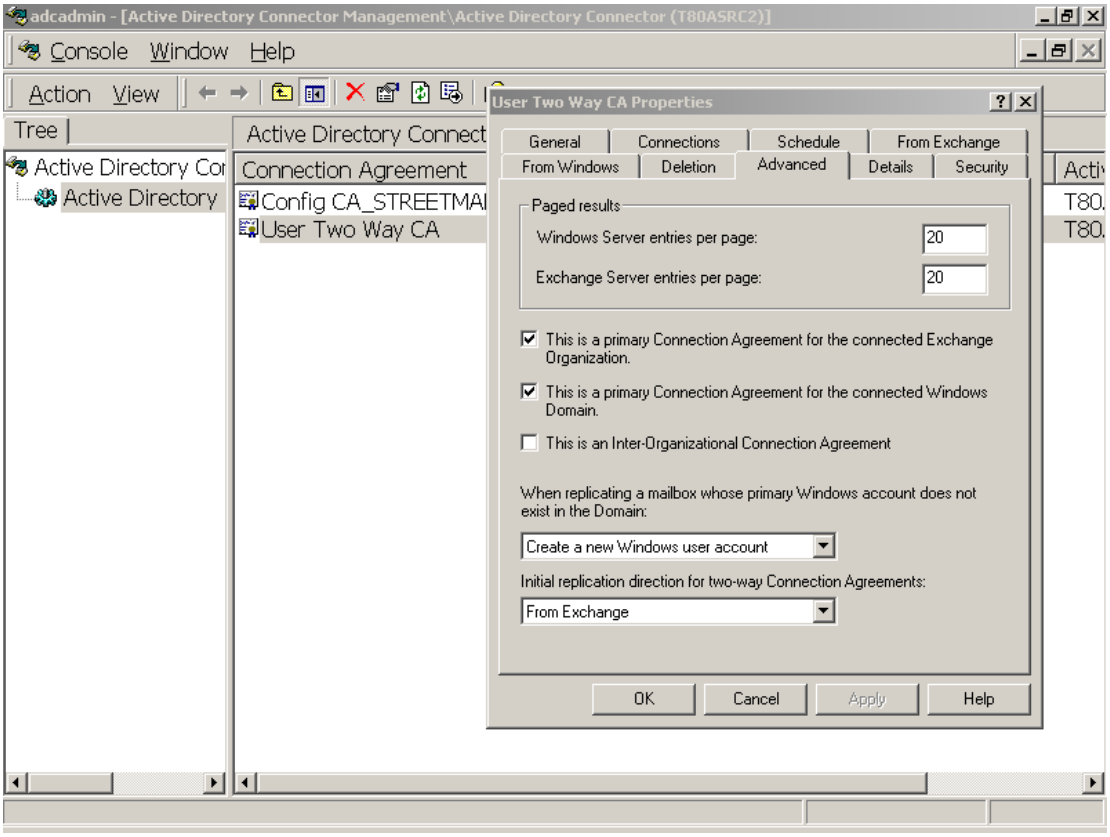
Table 2 describes the features of Active Directory objects that are mail-disabled, mail-enabled, or mailbox-enabled.

Active Directory Connectors

Active Directory Connector (ADC) provides a method for replicating a Microsoft Exchange Server version 5.5 directory with the Microsoft Windows 2000 Server Active Directory. Depending on how the Active Directory Connector Management is configured, the ADC can replicate containers in the Windows 2000 Active Directory to equivalent containers in the Exchange Server directory.

Conversely, the ADC can replicate selected Exchange directory containers into equivalent Windows 2000 Server Active Directory containers.

The administrator needs to have an ADC and multiple Connection Agreements can be set up. The figure shows an agreement between a Windows 2000 server and an Exchange 5.5 based server. There can be an agreement that runs every day at a certain time to update the Windows 2000 contacts to the Exchange 5.5 directory and another agreement to update the Windows 2000 AD from the Exchange 5.5 directory continuously.



In the figure, the two-way Connection Agreement was checked so that there is an option to add Exchange mailboxes when creating new users in Active Directory Users and Computers. A one-way Connection Agreement form Exchange to Windows will not provide the option to add a mailbox for the user because one already exists.

The administrator can choose to use any of the following for authentication between the two servers.

- Windows Challenge/Response
  Enable authentication using Windows network security.
- Windows Challenge/Response using Secure Sockets Layer (SSL)
  Enable authentication using Windows network security through an SSL-encrypted channel.
- Basic (Clear Text) using SSL

As the ADC uses LDAP as the directory services protocol, the Exchange Directory store has to be version 5.5. The Exchange 5.5 supports read/write of directory services. The replication mechanism is based on the last known Update Sequence Number (USN).

Extension of the Active Directory Schema in Exchange

Exchange extends Active Directory by adding auxiliary classes. The schema in Active Directory can be viewed by using the Active Directory Service Interfaces (ADSI) edit tool in Windows 2000 Support Tools. Active Directory includes entries specific to Exchange. Some of these entries include: Mail-Recipient Auxiliary Class, which enables e-mail and mailboxes on an object and provides e-mail addresses, protocol settings, and others; The Mail-Storage Auxiliary Class, which enables mailboxes for users and provides store quotas, homeMDB, deleted-item retention, and others. When an administrator creates a new user in Exchange, a message asks if the user is to be mailbox-enabled. The administrator can also enable the user later.

Attribute	**LDAP Attribute Name**	**Standard Active Directory (in GC)**	**After Exchange 2000 Installation (in GC)**
First Name	GivenName	No	Yes
Initials	initials	No	No
Last Name	surname	No	No
Display Name	Cn	No	Yes

Alias Name			
Mailing Address	Street	No	Yes
City		No	No
State	St	No	Yes
ZIP Code	Postalcode	No	No
Country	Co	No	No
Department	Department	No	No
Office	Physical DeliveryOfficeName	No	Yes
Telephone	TelephoneNumber	No	Yes
Fax	FacsimileTelephoneNumber	No	No
Home Telephone	HomeTelephone	No	No
Manager	Manager	Yes	Yes
SMTP Address	Mail	No	Yes
Custom Attributes	ExtensionAttributexx	No	No

Table 3 shows the schema modifications chart.

Administrators can also use Exchange Management Object to develop using Microsoft Visual Basic®; Visual Basic, Scripting Edition; or C++ to customize the administration. This provides a method of accessing Active Directory aside from using ADSI. The administrator can automate tasks such as moving users from one storage group to the other when the size of the storage group passes a certain limit.

This is demonstrated by an example of an application that references Exchange Management Object. Methods associated with the mailbox object also include move, remove, and create.

```
Sub CDOCreateMailBoxRecipient(Servername As String, _
                      DomainName As String, _
                      emailname As String, _
                      FirstName As String, _
                      LastName As String)

Dim objPerson As New CDO.Person
Dim objMailbox As CDOEXM.IMailboxStore
objPerson.FirstName = FirstName
objPerson.LastName = LastName
objPerson.Fields("userPrincipalName") = LastName
objPerson.Fields("userAccountControl") = 512
objPerson.Fields("userPassword") = "password"
objPerson.Fields.Update
objPerson.DataSource.SaveTo "LDAP://" + Servername + _
                     "/CN=" + emailname + _
                     ",CN=users," + DomainName

Set objMailbox = objPerson
tempstr = "LDAP://" + Servername + _
                   "/CN=newmailboxstore" + _
                   ",CN=First Storage Group,CN=InformationStore,CN=" + _
                   Servername + _
                   ",CN=Servers,CN=First Administrative Group," + _
                   "CN=Administrative Groups,CN=First Organization," + _
                   "CN=Microsoft Exchange,CN=Services," + _
                   "CN=Configuration," + DomainName
objMailbox.CreateMailbox tempstr
objPerson.DataSource.Save
End Sub
```

Table 4 shows the code for creating a mailbox on the information store by using the CreateMailbox method found in the Imailboxstore interface.

KERBEROS

Introduction

Kerberos is the fundamental security protocol in Windows 2000. It is provided natively within the Windows 2000 domain and integrated into the administrative and security model. Hence the administrator does not need to learn additional administrative tools to manage the infrastructure.

Kerberos identifies the client through secured means to a key domain controller. When the user logs on, it authenticates to the key distribution center (KDC). The KDC issues a ticket granting ticket. The client then uses the ticket granting ticket to access a service. A client who has the ticket to access the service can simply present the ticket for subsequent users. All of the tickets are encrypted through public key technology, which is more secure than secret key encryption.

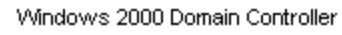


Figure 2 shows the steps involved in Kerberos authentication with the Windows 2000 domain controller and member and store server.

Kerberos and Exchange

In such an environment, Exchange 2000 is treated like a service. When the client needs to access Exchange, the client requests an Exchange service ticket from the KDC in the Windows 2000 domain controller. The service ticket is then used for authentication with the Exchange 2000 store server. For subsequent access to Exchange 2000, the client uses the service ticket and authentication is faster.

The Exchange service also uses Kerberos to make a service logon to the domain controller through the local system account. The local system account uses computer credentials, which consist of the account and password that is automatically changed every seven days. This provides better security compared with Exchange 5.5, which uses a site service account. The user name of the Exchange 2000 server is added to the Exchange Servers Group, which is added to the access control list (ACL) of the core objects.

If a client has already authenticated to server X, and server X needs to request another server Y running on another computer, server X can request for the ticket on behalf of the client. This is possible because Kerberos supports authentication delegation. Authentication across different domains is also possible, provided there is a trust relationship. It should also be noted that while trust is transitive for the computers in the same domain, for external domains and non-Windows systems, they are not transitive. They have to be explicitly set.

Kerberos delegation is a property that can be set on the account and computer. The fact that the account is trusted for delegation means that any computer can forward the credentials of the account. A computer is trusted for delegation means that the computer can forward credentials to any other computers.

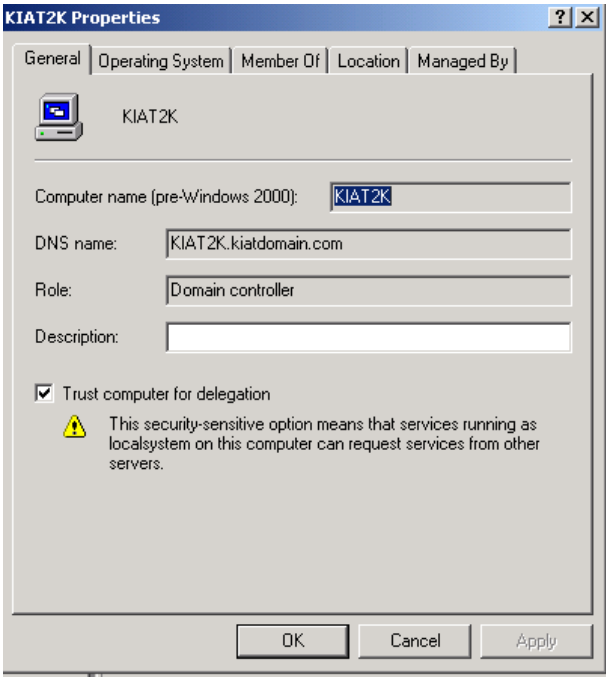


Figure 3 shows a snapshot of the configuration for the server specifying that the computer can be trusted for delegation.

Authentication delegation in Exchange

An example of how authentication delegation is used in Exchange implementation is in multi-tier Outlook Web Access. The Windows 2000 IIS 5.0 and Exchange 2000 Store Server are on separate computers in the same domain. The client needs to identify itself to the KDC and using a forwardable flag on the ticket to the Windows 2000 IIS 5.0 server, the client is authenticated through delegation when IIS needs to access the Exchange 2000 store on another computer. The ticket that IIS used has the authorization data of the user, not IIS. This is an improvement over NTLM, which does not support forwarding of credentials.

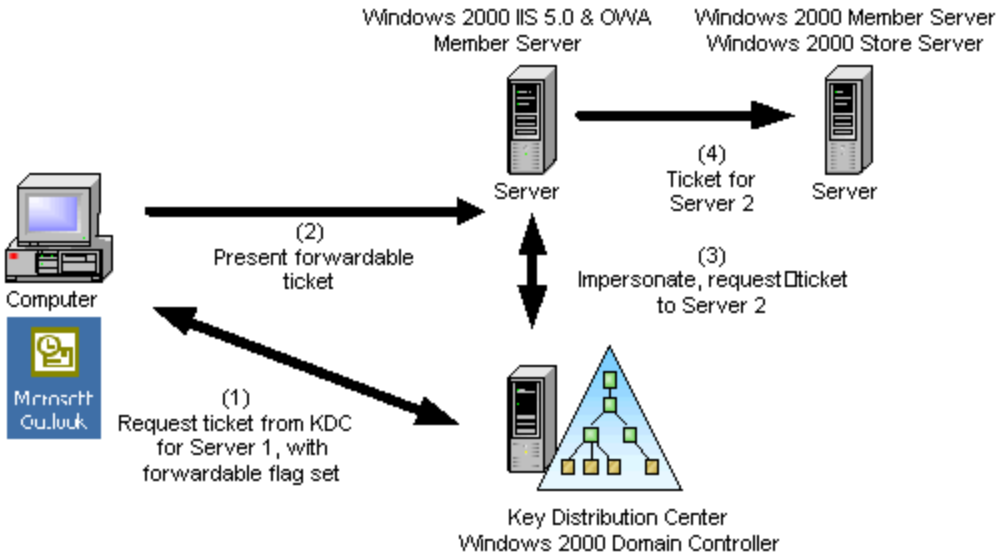


Figure 4 shows how Exchange 2000 uses authentication delegation. The Member and Store Server trusts the ticket sent and acknowledges that the user will be logging on to the server.

Kerberos for non-Windows 2000 clients

Clients with Kerberos support are Windows 2000 Professional. For Windows 95 and Windows 98, Kerberos add-ons are available. However, these add-ons are not available for Windows NT.

Best Practices

Timing is important in Kerberos because it uses a time stamping system to eliminate Windows NT replay attack. Windows 2000 comes with a time service (SNTP). A Domain Name Service (DNS) that resolves domain names and services to IP addresses is needed by Kerberos in mutual authentication and referral processes.

If the time or date is not synchronized between your computer and the domain to which you are attempting to log on, the following error message will occur:

> The system cannot log you on due to the following error:
> There is a time difference between the Client and Server.
> Please try again or consult your system administrator.

Although a Windows 2000 Kerberos Authentication package is the default in Windows 2000, it coexists with challenge/response (NTLM) and is used in instances in which both a client and server can negotiate Kerberos.

Finally, Kerberos is intranet LAN-oriented because it needs a domain controller and has a client load. It is recommended to limit the number of domains to cut down the inter-domain referrals.

ACCESS CONTROL

Access Control Model

When a user logs on to a Windows 2000 system, the system authenticates the user's account name and password. If the logon is successful, the system creates an access token. Every process executed on behalf of this user will have a copy of this access token. The access token contains security identifiers that identify the user's account and any group accounts to which the user belongs. The token also contains a list of the privileges held by the user or the user's groups. The system uses this token to identify the associated user when a process tries to access a securable object or perform a system administration task that requires privileges.

In Windows 2000, each object has a set of security information, or security descriptor, attached to it. Part of the security descriptor specifies the groups or users that can access an object, and the types of access (permissions) granted to those groups or users. This part of the security descriptor is known as a Discretionary Access Control List (DACL). If a Win32 object does not have a DACL, the system allows everyone full access. If an object has a DACL, the system allows only the access that is explicitly allowed by the Access Control Entries (ACEs) in the DACL. If there are no ACEs in the DACL, the system does not allow access to anyone. Similarly, if a DACL has ACEs that allow access to a limited set of users or groups, the system implicitly denies access to all trustees not included in the ACEs.

Access Control Model used in Exchange 2000 follows that of Windows 2000 and is completely different from Exchange 5.5. Hence there is more granularity in the access control model in Exchange 2000 compared to Exchange 5.5. In Exchange 5.5, access control is based on container-level grant while in Exchange 2000, grant or deny can be set by container, item, and property level. Also, Exchange 2000 objects are based on the Windows NT File System (NTFS) and Active Directory Objects. SID Objects replace the Mail-based objects. Security evaluation is based on ACEs.

An example is the property ACEs of the public folder. Notice the granularity of the permission settings. The user1 is given read permission to the object only while an enterprise has full control to the object and subcontainer.

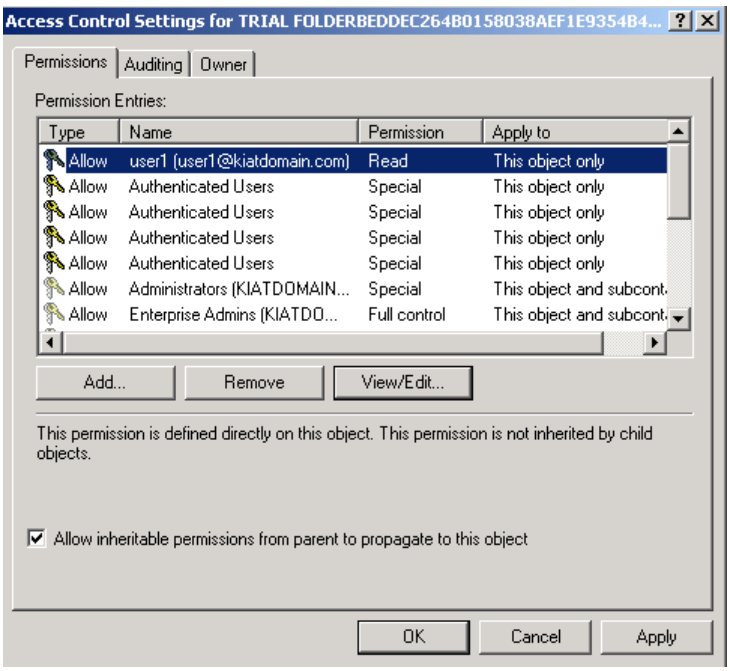

Access Control Settings for TRIAL FOLDERBEDDEC264B0158038AEF1E9354B4...
Permissions
Auditing
Owner
Permission Entries:
Type
Name
Permission
Apply to
Allow user1 (user1@kiatdomain.com) Read This object only
Allow Authenticated Users Special This object only
Allow Authenticated Users Special This object only
Allow Authenticated Users Special This object only
Allow Authenticated Users Special This object only
Allow Administrators (KIATDOMAIN... Special This object and subcont
Allow Enterprise Admins (KIATDO... Full control This object and subcont
Add...
Remove
View/Edit...
This permission is defined directly on this object. This permission is not inherited by child objects.
Allow inheritable permissions from parent to propagate to this object
OK
Cancel
Apply

Figure 5 Depending on the type of object, the administrator can specify what actions can be carried out. For instance, user1 cannot create an object in the object, subcontainer, and children, but can list contents in the object and subcontainers. Authenticated users can have specific special permissions, which can be further defined.

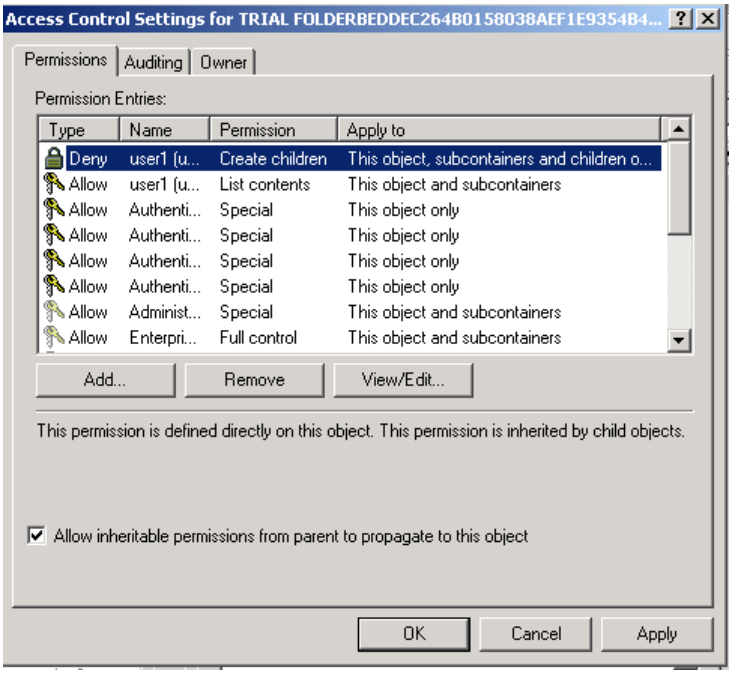

Access Control Settings for TRIAL FOLDERBEDDEC264B0158038AEF1E9354B4...
Permissions
Auditing
Owner
Permission Entries:
Type
Name
Permission
Apply to
Deny user1 (u... Create children This object, subcontainers and children o...
Allow user1 (u... List contents This object and subcontainers
Allow Authenti... Special This object only
Allow Authenti... Special This object only
Allow Authenti... Special This object only
Allow Authenti... Special This object only
Allow Administ... Special This object and subcontainers
Allow Enterpri... Full control This object and subcontainers
Add...
Remove
View/Edit...
This permission is defined directly on this object. This permission is inherited by child objects.
Allow inheritable permissions from parent to propagate to this object
OK
Cancel
Apply

Figure 6 Inheritance of ACL can be controlled. Inheritance is the settings flow down from parent object to child object. For instance, inheritance can be restricted to one level or child and can be protected from the parents by unchecking the box for the

Allow inheritable permissions from parent to propagate to this object in the necessary objects.

Item Level and Property Level

Effectively the granularity of the access control in Windows 2000 can provide Exchange 2000 with the following:

- Item Level ACEs.

  If a user has access to only five out of the ten items in a public folder, the user would only see five of the ten items.

- Property Level ACEs.

  When a user who does not have access rights to certain attributes does a search, the user would have only the results that he or she can access.

However, important issues related to the new access control model includes the following that in particular affects the public folder system:

- As public folders are migrated from Exchange 5.5, the distribution lists become distribution groups, which do not have SIDs. In the beta version of Exchange 2000, there is an additional administrative task for creating groups based on distribution lists in Exchange 5.5 and adding them to the ACLs manually.
- Public folders with the new ACLs from Windows 2000 to be replicated to the Exchange 5.5 system have to be tested for their access control functions.

Planning Considerations

With a detailed access control model, the user has to take into consideration the following factors:

- Resources that require separate permissions. This is done by setting policies specifically for those particular resources or group of resources.
- Using property-level permissions to make an object behave a certain way to certain users. For instance, the e-mail address of an intern can only be read by the team but not by everyone.
- Permissions are best applied at the highest possible level of hierarchy. For instance, with a planned folder hierarchy of many layers, it is easier to let each folder inherit the permissions. However, for specific folders with special requirements, inheritance can be turned off.

Directory-Level Delegation

Property-based ACEs, object type-based ACEs, and fine-grain inheritance controls enable the delegation of administration to a certain group of SIDs in Active Directory. Delegation can take place in two levels. These are Directory-level delegation and Exchange 2000 Infrastructure-level delegation. Directory-level delegation is carried out through the unification of Windows 2000 and Exchange 2000 and a delegation wizard. To carry out delegation on the organization unit level, use the Active Directory Users and Computers snap-in. For instance, directory-level delegation allows a manager in a location to reset the password and one level lower, the Legal and Human Resources (HR) groups to manage the Legal and HR groups. The Exchange 2000 Infrastructure-level delegation takes place in the Exchange system management snap-in. For instance, in the public folder, we can specify a certain group of administrators to be allowed to create folders while another group of administrators to create single-level child folders in the folder. These demonstrate the flexibility of the delegation.

Delegation of Control Wizard
Completing the Delegation of Control Wizard
You have successfully completed the Delegation of Control wizard.
The groups, users, or computers to which you have given control are:
Creator Group (CREATOR GROUP)
They have the following permissions:
Full Control
For the following object types:
Administrative Groups Container
To close this wizard, click Finish.
< Back
Finish
Cancel

Figure 7 shows the delegation wizard in which the administration group container objects can delegate the administration to creator group with full control permissions.

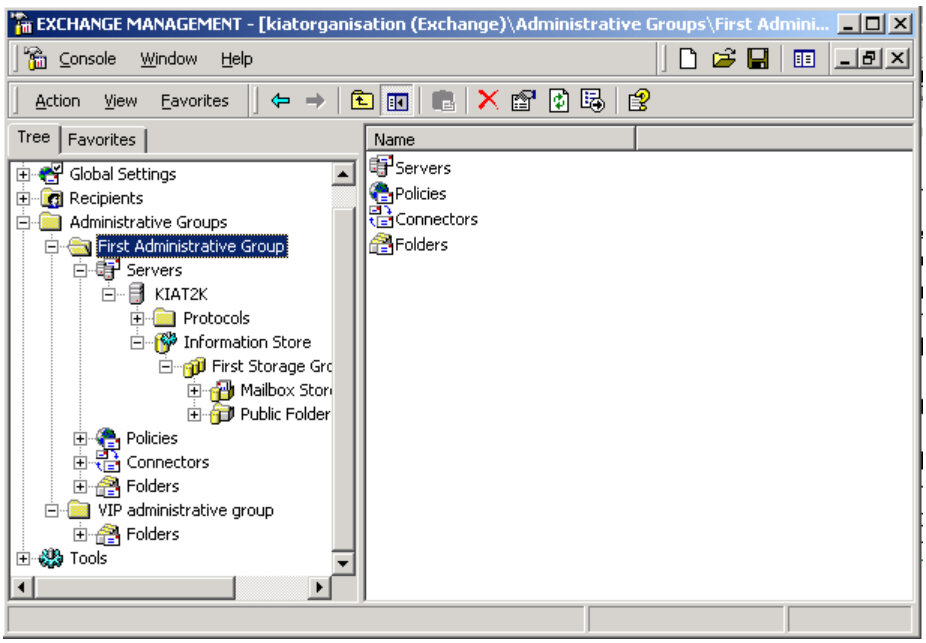


Figure 8 shows that different administrative groups can be created. There may be a group of administrators that look after the VIPs in a company and the VIPs have their own policies regarding the mailbox store. The administrative groups are not shown by default and are shown by enabling the **Display administrative groups** in the Organization properties.

The administrator can use delegation by using:

- Windows GUI-based customized Microsoft Management Console (MMC) snap-in or taskpad
- Web-based administrative interface using ASPs
- Script-based using Windows Scripting Hosts (WSH) and Active Directory Service Interface (ADSI)

Delegation can be done on groups with SIDs. However, delegation cannot be done on mail groups' distribution lists, as they do not have SIDs. Hence delegation can only be done on security groups. Also, it depends whether the environment is mixed or native mode. In a mixed mode environment, there is no universal group and cannot nest groups within one another.

The table shows the different security group types and features. There are four basic security group types: universal, global, domain local, and local. User scope shows where in the forest the group can be used. A universal group can contain the forest and be defined in the AD-GC. The global group is defined in the AD-GC but not the membership. The difference from Windows NT 4.0 is the use of a universal group, which puts the global group into the ACL of the domain local group of another domain by putting the global group in the universal group and

putting the universal group in the domain local group. Nesting can only be done in a native mode environment.

Type	Usage Scope	Content Scope	Defined in
Universal	Forest-wide	Forest	AD-GC(group & membership)
Global	Forest-wide	Domain	AD-GC(group only)
Domain Local	Domain	Forest	AD-Domain
Local	Local Computer	Forest	SAM

Exchange Roles

A role is a link that contains the SID and the Exchange 2000 rights. They are essentially resource groups for Exchange 2000 administration. These roles are not defined in the directory but rather in the Exchange 2000 stores. These roles are application driven and customizable by the developer. A developer can define roles as part of the application design and then populate at deployment time with actual users and groups. In an Exchange 2000 public folder store, the Role-ACEs refer to the roles defined in the Exchange 2000 store. These roles are evaluated at run-time and the security system of the store query the role definition table for the contents of the role when the user accesses the public folder. Hence the changes in the roles are instantly updated.

These changes in the access level control are reflected in the Exchange 2000 public folder ACEs interface. User level permissions, default message permissions, permissions on the active directory object, and administrative permission on the objects contained in the store can be set.

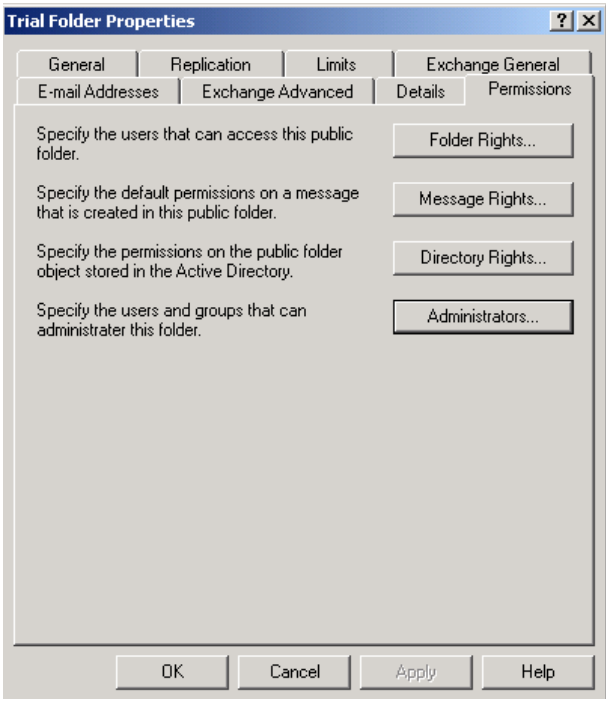


Figure 9 shows the permission settings for the **trial folder**. Note the different specifications for different parts of the folder and the granularity of the access control.

CERTIFICATE SERVICE

Microsoft Certificate Service is a certificate authority product available in Windows 2000 and is integrated with Active Directory. This server provides public key infrastructure for not only Exchange servers but also other applications like browser, IPSEC and Encryption File System (EFS). As can be seen from the snapshot of the certificate service MMC, the administrator can choose the type of certificates to be issued. Depending on the functions, different certificates are issued. These certificates can also be easily revoked if there is, for instance, a compromise of security.

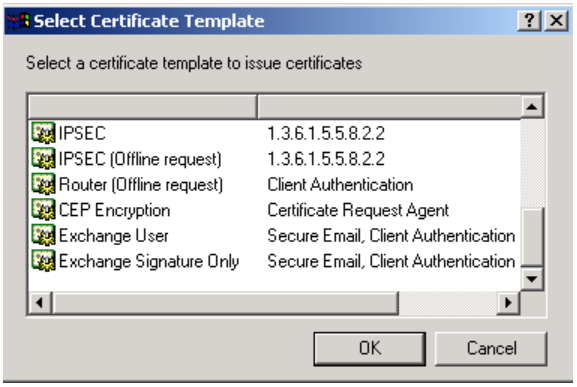


Figure 10 shows the different applications that use the certificate provided by the Certificate Service. Note that Exchange uses certificates for both encryption and signature.

Certificate Service and Active Directory

The user property page contains per-user security functions: enable, revoke, and recover. The Certificate Service supports forty levels of hierarchy and can be a subordinate to any third party CA. Active Directory maintains a list of all the organization certificate servers. Each time a Windows 2000 computer boots and every 24 hours thereafter, all certificates are downloaded and added to the root store (used by Schannel SSPI to hold trusted certificates). On the other hand, applications on non-Windows 2000 servers using certificate services have mechanisms to check for revoked certificates.

Certificate Service and KMS

Certificate Service is being used by the Exchange 2000 Key Management Service (KMS) to provide security on the application layer of the messaging system. It produces X.509v3 user certificates that are used by Exchange and Outlook for digital signature and encryption. The X.509v3 user certificates are recognized by

Secure/Multipurpose Internet Mail Extension (S/MIME) clients and ensure interoperability among different clients when used across an Internet.

The Enroll Agent (Computer) policy of the CA has to be enabled before the KMS is installed. To start using KMS, the administrator can specify that two different people must be present with their password before the system can be activated (Missile SILO style multiple password policy). The administrator can also choose to use the different types of encryption algorithms and hash functions. Two sets of certificates are generated for each user. One is for encryption and another is for signing. The user's private key is stored in an encrypted .EPF file in Pre-Outlook 98, an Internet Explorer (IE) protected store in Outlook 98, and in the registry for Outlook 2000. The public key is stored in Active Directory. When this secured function is implemented, messages that are sent can be encrypted and signed thus providing privacy, authentication, and no repudiation.

However, in an enterprise system, issues regarding maintenance and implementation are a concern. Implementing security enhancements like encryption at the application layer means that only the users who are supposed to gain access to information have done so. Applications have to be easy to use and support. Exchange 2000 has enhancements such as allowing mailboxes to be moved easily, having different admin groups, and others. Exchange 2000 KMS is designed with these enhancements in mind.

Previous versions of KMS restrict KMS to just one per site. However, in Exchange 2000 KMS, it fits the site-based model. The KMS organizational unit becomes the Admin Group and each new admin group created allows KMS to be installed or pointed to an existing KMS. The administrator can also enroll the users in bulk by groups, selected users or server.

In the previous version of KMS, to move a user from one site to another, the administrator had to provide solutions such as requesting the user to decrypt existing messages and other workarounds. If a user moved to a new site with a new KMS, the old keys could not be recovered. In Exchange 2000, the users can now be exported from one KMS to another new one. To ensure security, the administrator has to specify the destination of the new location before he or she can export the users.

Also KMS is no longer tied to a single Certificate Server. The Certificate Server certificates are trusted throughout the organization and are available for users to enroll. Since KMS is no longer tied to a single Certificate Server, rollover functions are not needed.

Administrators should also note that upon implementing encryption on the application layer, content filtering or virus checking across gateways is compromised. The organization has to take this into consideration.

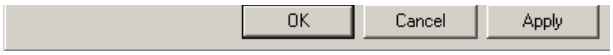


Figure 11 shows the properties in the Advanced Security configuration of Exchange System Management. The Security administrator can choose to distribute the token through e-mail or hand carry it. For backward compatibility issues, administrators can specify the certificate version.

Figure 12 shows what the configuration of the Outlook client will look like. The user is guided through the steps to carry out enrollment, such as entering the token and specifying where to get the digital identification.

NOTE: Advanced security cannot be applied to Outlook Web Access because it requires an executable to run on the browser, which is currently not possible. Hence, non-Microsoft clients have to use third party software. An example is NEXOR Defender, which is used on UNIX, for the DMS.

IP SECURITY (IPSEC)

While Key Management Service provides security on the application layer, IPSEC provides security on the IP transportation layer (Network Layer 3). This enables protection with low overhead and can be deployed in different scenarios, such as workgroup, LAN, and remote access. Also, it provides protection in the IP and upper-layer protocols in the TCP/IP protocol suite, such as TCP, UDP, ICMP, and other protocols that sends traffic at the IP layer.

IPSEC uses the Diffie-Hellman algorithm to enable key exchange, and provides the keying material for all other encryption keys. IPSEC can automatically generate new keys during a communication. The communication can be sent in blocks of data, each block secured with a different key. This prevents an attacker from obtaining the entire communication with a single compromised key.

IPSEC and SSL

Other security mechanisms that operate above Network Layer 3, such as the Secure Sockets Layer (SSL), can only provide security to applications that understand and know how to use SSL. An example of such an application is the Web browser. All other applications must be notified to protect communications with SSL. Security mechanisms that operate below Network Layer 3, such as link layer encryption, only protect the link, but not necessarily all links along the data path. This makes link layer encryption unsuitable for end-to-end data protection on Internet or routed intranet scenarios.

Using IPSEC in LAN

IP Security (IPSEC) defines protocol for network encryption at the IP protocol layer (Network Layer 3). The default IPSEC authentication is Kerberos. However, if Certificate Service is made available, each domain member will have the appropriate certificate installed. Another method besides using Kerberos or Certificate Service is to use a pre-shared key. This is a simple method for authenticating computers not based on Windows 2000 or Kerberos.

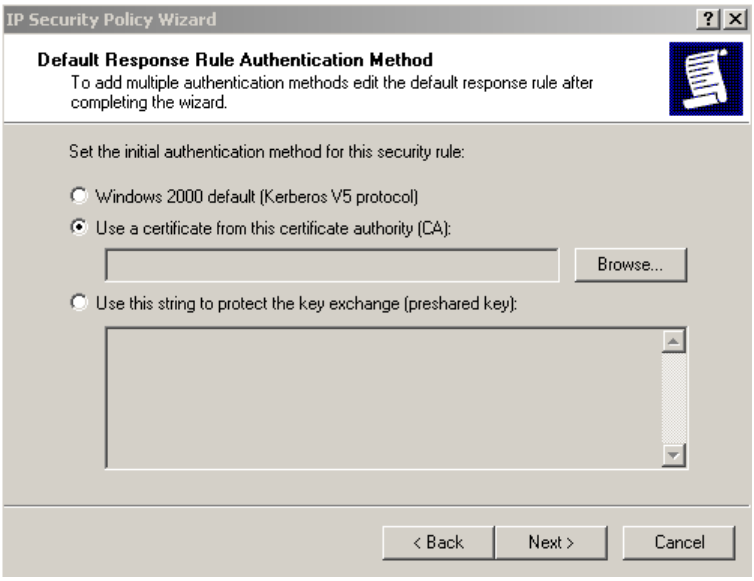

IP Security Policy Wizard
Default Response Rule Authentication Method
To add multiple authentication methods edit the default response rule after completing the wizard.
Set the initial authentication method for this security rule:
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
< Back
Next >
Cancel

Figure 13 shows the IP security policy created and the administrator can specify the authentication method for the security rule.

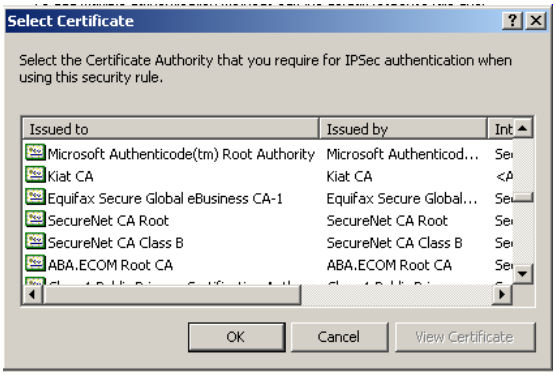


Figure 14 shows the different certificates that can be used. The system comes with a list of certificate authority that can be used.

IP Security policies can be set according to the Active Directory units. From the Group Policy Objects, which can be linked to site, domain, or organizational unit in Active Directory, the type of security policy is assigned. There are three predefined policies:

- Security responder

  The client is assigned to the domain group.

  This is a security policy to ensure that these computers can respond to requests for secure communications as required.

- Security Initiator

  The server can communicate securely but may need to communicate with computers, which cannot respond to secure requests.

- Lockdown

  A secure server ensures that incoming, unsecured communications are rejected. However, due to the strictness of the policy, exemptions have to be added for special traffic types such as SNMP traffic (IPFilter list UDP to & fro 161 and to & fro 162). An additional point to note is that if DNS names are used, DNS servers are not IPSEC-enabled, then enabled mirrored, TCP from & to 53.

IPSEC and Exchange

IPSEC provides security on a different level than KMS. In an environment that plays emphasis in this area will use IPSEC for network from client to server and even server to server. This can take place in a LAN. However, in an organization that needs to use Virtual Private Network (VPN) or Remote Access Service (RAS), IPSEC can also be used. In Windows 2000, there are two types of tunneling protocol: Point-to-Point Tunneling (PPTP) and Layer 2 Tunneling Protocol (L2TP). The former uses the Microsoft Point-to-Point encryption (MPPE) to encrypt the Point-to-Point Protocol (PPP) while the later is used together with IPSEC as L2TP over IPSEC. L2TP is a draft Request for Comments (RFC)-based protocol and has two layers of encryption being used: L2TP and IPSEC.

Figure 15 shows the options available for the Virtual Private Connection (VPN). L2TP and PPTP are available.

OTHER SECURITY ENHANCEMENTS

Encrypting File System (for the client PC)

The Encrypting File System (EFS) is a feature of Windows 2000 that allows users to encrypt data directly on volumes that use NTFS. It operates by using certificates based on the X.509 standard. If no certificate authority (CA) is available from which to request certificates, the EFS subsystem automatically generates its own self-signed certificates for users and default recovery agents.

The EFS supports transparent encryption and decryption of files stored on a disk in NTFS. A recovery policy is automatically implemented when users encrypt a file or folder for the first time. This ensures that users who lose their file encryption certificates and associated private keys are able to use a recovery agent to decrypt their files.

The user must understand that once the encrypted file leaves the hard disk, it is not encrypted. When a user sends a file as an attachment, the file will not be encrypted. This is different from using the advanced security features of Exchange with KMS. The encrypted file system encrypts files on the hard disk and when the directory is opened for sharing, the files cannot be read.

However, when a user is running an application that retrieves a file from the hard disk as the legitimate user, the file is decrypted. It should be clear that the EFS only address the encryption of data on disk. When data is transferred over the network, it will need IPSEC, SSL, and others to ensure that data is encrypted over the network.

The EFS is useful for mobile users who can encrypt directories, such as personal mail folders. In this way, if their portable computer is lost, the data cannot be read. For organizations that do not want this feature, a security policy can be set through Active Directory Users and Computers. (refer to KB Q222022)

Figure 16 shows the file encryption options available in Windows Explorer.

Auditing in Windows 2000

Auditing gathers security relevant information. Two tools available are event viewer and security configuration analysis. Event Viewer in Windows 2000 is extended to include the directory service, DNS service, and file replication service. The security configuration and analysis tool allows administrators to analyze the security of the system and reapply it. The security configuration analysis is based on the templates defined to be analyzed and applied to the computer. The administrative tool is also a snap-in.

The security template is a set of predefined settings in terms of account policies, local policies, restricted groups, registry, file system, and system services. The settings are also classified into basic, compatible, secured, highly secured, and dedicated domain controller templates. These templates are later used to configure the security configuration analysis. The analyzer in the security configuration analysis is run to show whether there are discrepancies in the settings and templates. This is useful to check if security policies are implemented and serve as another form of audit checking.

This application has to be run on the local computer. But there is a command prompt Secedit to cater for batch jobs to be run.

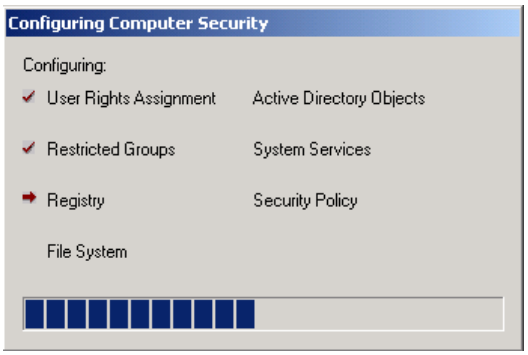


Figure 17 shows the different areas checked by the security configurator and analyzer.

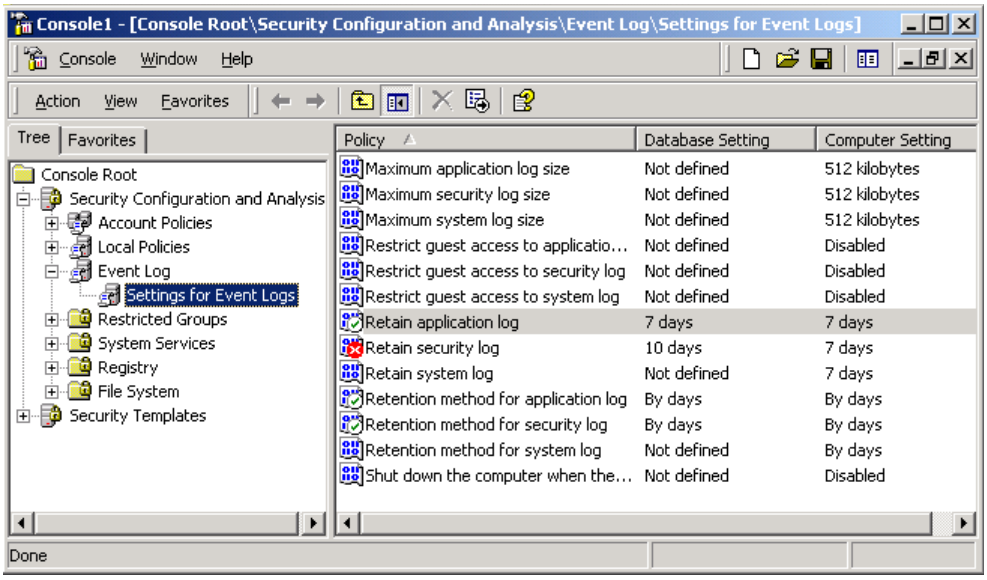


Figure 18 shows the result of the analysis that indicates the discrepancy found in the configuration. Under the retain security log portion, the computer settings have been fixed on seven days, but the administrator has instead set them to ten days, which could be a violation of the policies.

FINAL NOTES

The administrator has to understand the different options available to enhance the overall security of the infrastructure. In an enterprise where different platforms are available, it is necessary to also understand the level of security that can be implemented without causing interoperability issues. These features found in Windows 2000 Advanced Server and Professional provide a secure environment for messaging and collaboration with Exchange 2000.

Aside from adding the security features and configuring them properly, Exchange Server also allows enterprise administrators to place security rules. For instance, Exchange 2000 comes with virtual servers for different protocols and caters or protocol logging. Within a Simple Mail Transfer Protocol (SMTP) virtual server, SMTP can be configured to place restrictions on relay e-mail, control connection, the number of connections, and forwarding mail to bastion hosts.

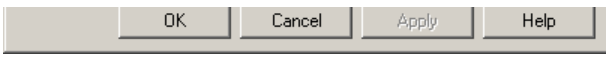


Figure 19 shows the configuration options for the SMTP virtual server. Notice the different controls and restriction configurations available.

Two Broad Areas of Security

Security Within LAN

The first step toward enhancing security is to understand the components required. With Windows 2000 and Exchange 2000, Active Directory plays an important role not only providing the directory for Exchange 2000, but also providing an environment for PKI. Certificate Services play an important role in certificates for Kerberos, KMS, EFS, IPSEC and SSL. The management can then implement security on different layers of the network stack, on the network layer with IPSEC, and on the application layer with KMS.

With the granular access control in Windows 2000, the organization can have different administrators doing different tasks on Exchange, Certificate Services and Directory services. They can only handle the jobs within their access rights. The security configuration and analyzer can also be used to ensure that security policies are adhered to.

External Security

Exchange 2000 is designed with connection to the Internet in mind. SMTP is the core mail transport agent, and other collaborative features such as Instant Messaging Service and NetMeeting services are available. From the infrastructure point of view, has to be in place to meet these initiatives. Here we treat any cloud that is not within the LAN as external, thereby not restricting to just the Internet.

PORTS and PROTOCOLS used

A firewall or proxy server fundamentally separates one network from the other. A common scenario is the connection of the LAN to the Internet. They range from a simple packet filter to complex bastion hosts that analyze traffic for each application type. The following is a list of protocols and ports used by

Windows 2000 servers and Exchange 2000 servers. It is important to go through them to customize the firewall that you are using.

PORT	TCP/UDP	NAME OF SERVICE
42	TCP	WINS Replication
47	TCP	GRE for PPTP
53	UDP	DNS Name Resolution
53	TCP	DNS
67	UDP	DHCP Lease (BOOTP)
68	UDP	DHCP Lease
88	UDP	Kerberos
135	TCP	Location Service · RPC · RPC EP Mapper · WINS Manager · DHCP Manager · MS DTC
137	UDP	NetBIOS Name Service · Logon Sequence · Windows NT 4.0 Trusts · Windows NT 4.0 Secure Channel · Pass Through Validation · Browsing · Printing
137	TCP	WINS Registration
138	UDP	NetBIOS Datagram Service · Logon Sequence · Windows NT 4.0 Trusts · Windows NT 4.0 Directory Replication · Windows NT 4.0 Secure Channel · Pass Through Validation · NetLogon · Browsing · Printing
139	TCP	NetBIOS Session Service · NBT · SMB · File Sharing · Printing · Logon Sequence · Windows NT 4.0 Trusts · Windows NT 4.0 Directory Replication · Windows NT 4.0 Secure Channel · Pass Through Validation · Windows NT 4.0 Administration Tools (Server Manager, User Manager, Event Viewer, Registry Editor, Diagnostics, Performance Monitor, DNS Administration)
389	TCP/UDP	LDAP
500	TCP/UDP	ISAKMP/Oakley negotiation traffic (IPSEC)

522	TCP	User Location Store
636	TCP/UDP	LDAP (over TLS/SSL)
750	UDP	Kerberos Authentication
750	TCP	Kerberos Authentication
751	UDP	Kerberos Authentication
751	TCP	Kerberos Authentication
752	UDP	Kerberos Password Server
753	UDP	Kerberos User Registration Server
754	TCP	Kerberos Slave Propagation
888	TCP	Logon and Environment Passing
Dynamic	TCP	Directory Replication
1109	TCP	POP with Kerberos
1723	TCP	PPTP Control Channel (IP Protocol 47 – GRE)
2053	TCP	Kerberos de-multiplexor
2105	TCP	Kerberos encrypted rlogin
3268		Global Catalog
3269		Global Catalog
3389	RDP	Terminal Services

Table 5 shows the Ports and the Protocols for the services in Windows 2000.

PORT	TCP/UDP	NAME OF SERVICE
25	TCP	SMTP
80	TCP	HTTP
102	TCP	MTA – X.400 over TCP/IP
110	TCP	POP3
119	TCP	NNTP
135	TCP	· Client/Server Communication · RPC · Exchange Administration
143	TCP	IMAP
389	TCP	LDAP
443	TCP	HTTP (SSL)
465	TCP	SMTP (SSL)
563	TCP	NNTP(SSL)
636	TCP	LDAP (SSL)
993	TCP	IMAP4 (SSL)
995	TCP	POP3 (SSL)
1720	TCP	H.323 CALL SETUP
1731	TCP	AUDIO CALL CONTROL
2980	TCP/UDP	INSTANT MESSAGING SERVICE
Dynamic	TCP	H323 CALL CONTROL
Dynamic	UDP	H323 CALL (RTP OVER UDP)

Table 6 shows the ports and services for Exchange 2000.

Remote Access And VPN

The Windows 2000 RAS and Routing and Remote Access Service (RRAS) offer security options that mobile users can use for safe Internet access to the LAN. They include the PPTP and L2TP.

Windows 2000, when used as a RAS server, can provide different authentication.

- Basic Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP), an authentication protocol used by remote access and Network and Dial-up Connections. Using CHAP, a remote access client can send its authentication credentials to a remote access server in a secure form. Microsoft has created a Windows-specific variant of CHAP called MS-CHAP.
- Extensible Authentication Protocol (EAP). An extension of PPP that provides remote access user authentication by means of other security devices. Support for a number of authentication schemes may be added. These schemes include token cards; dial-up; the Kerberos V5 protocol; one-time passwords; and public key authentication using smart cards, certificates, and others. EAP works with dial-up, PPTP, and L2TP clients. EAP is a critical technology component for secure VPNs because it offers more security against brute force or dictionary attacks (where all possible combinations of characters are attempted), and password guessing than other authentication methods, such as CHAP.

Lowest Common Denominator

With the various security features available, the administrator has to consider the lowest common denominator to ensure the operability of Exchange across different levels of security work. The following is a summary of some of the encryption and authentication used and the keys in U.S. and Canada. For other countries, it would be advisable to seek clarification from the Microsoft representative on the length of key permitted.

Services	Method used	US/CANADA
IPSEC	Encryption	DES 128-bit
	Authentication	MD5 128-bit
		SHA 160-bit
	Integrity	Kerberos
KMS	Encryption	DES, 3DES 128-bit

	Digital Signature	RSA 512-bit
EFS	Encryption	DESX 128-bit

FOR MORE INFORMATION

For the latest information about the Exchange 2000 and Windows 2000 technologies, visit the Microsoft Web site at:

http://www.microsoft.com/exchange/

http://msdn.microsoft.com/

Find more information on the port numbers at:

http://www.isi.edu/in-notes/iana/assignments/port-numbers